ABSTRACT OF THE DISCLOSURE

Approaches for preventing TCP data injection attacks in packet-switched networks are disclosed. A first approach provides for dropping received segments that carry ACK values smaller than the next unacknowledged sequence number expected minus the maximum window size. This approach helps keep spurious injected segments out of the TCP re-assembly buffer. In a second approach, heuristics are used to examine the sequence number of a newly arrived segment, and when the sequence number is the next expected, then the newly arrived segment is used and the contents of the re-assembly buffer are not considered. Further, if the data payload of the newly arrived segment overlaps in sequential order with segments already in the re-assembly buffer, the overlapped segments in the re-assembly buffer are considered spurious and are discarded. Thus, this approach helps remove spurious data from the re-assembly buffer if the first approach somehow fails to prevent the data from entering the re-assembly buffer.